

## **REMARKS**

Claims 1-26 are pending in the application. Amendments have been made to claims 1, 3-5, 11-15, 20, and 26. Support for these amendments can be found, *e.g.*, on page 13, line 14 and page 19, lines 7-15. No new matter has been added. Applicant respectfully requests reconsideration and allowance of claims 1-26.

### **Claim Amendments**

Claims 1, 14, 15 and 26 have been amended in order to clarify that the requesting party obtains the numerical identifier and the identity verifier from a transaction initiator claiming to be associated with the numerical identifier. Support for this amendment can be found, *e.g.*, on page 19, lines 7-15.

Claims 1 and 26 have been amended to clarify that the list of identity verifiers, and not only one identity verifier on the list, is linked to at least one unique numerical identifier. Support for this amendment can be found, *e.g.*, page 16, lines 9-10.

Claims 1 and 26 have also been amended to clarify that the list of identification verifiers linked to the numerical identifier is provided to the registered user. Support for this amendment can be found, *e.g.*, on page 13, line 14 and page 19, 7-11.

Further editorial revisions have also been made to the claims in order to correct grammatical and typographical errors, to conform to U.S. claim format, and to remain consistent with the specification.

Applicants note that none of these amendments are made to overcome an art rejection and, therefore, should not be construed as limiting.

### **Section 102 Rejections**

Claims 1-4, 11-21, and 23-26 have been rejected under 35 U.S.C. 102(b) as being anticipated by Heinz (U.S. 5,812,764, hereinafter "Heinz"). Applicant respectfully traverses the rejection.

Claim 1 recites, in part, a method of verifying the identity of a registered user. The method includes obtaining a list of at least two identity verifiers and linking the list of identity verifiers to at least one unique numerical identifier. The method further includes receiving a numerical identifier and an identity verifier from a requesting party, which obtained the

numerical identifier from a transaction initiator claiming to be associated with the numerical identifier. The method still further includes determining whether the received identity verifier is within the list of identity verifiers linked to the received numerical identifier. A registered user, therefore, can choose with which identity verifier to verify itself.

Claim 1 refers to the actions of three separate entities: (1) a verification system to perform the steps recited in claim 1; (2) a transaction initiator to claim to be associated with the numerical identifier; and (3) a requesting party to send the numerical identifier received from the transaction initiator to the verification system to verify that the transaction initiator is the registered user.

In contrast, Heinz discloses a password management system by which a server computer verifies that a client computer, which is attempting to log onto the server, is a registered user. The server computer contains a list of passwords for each registered user. Each password in the list corresponds with a particular password identifier. Each registered user has a copy of its respective list. When the server attempts to verify that a client computer is a registered user, the server sends a particular password identifier from the list associated with the registered user to the client. The client searches its copy of the list for the password associated with the particular password identifier and sends the password to the server. The server then verifies whether the password sent by the client matches the password associated with the particular password identifier. Control over which password is used, therefore, belongs solely to the server.

Heinz does not disclose or suggest determining whether the received identity verifier is within the list of identity verifiers linked to a received numerical identifier. Even if the server identifies the list associated with the registered user using a numerical identifier associated with the client computer, a point Applicant does not concede, the server in Heinz does not check whether the received identity verifier (*i.e.*, the password) is within the list associated with the registered user. Rather, the server merely determines whether the password is associated with the password identifier sent to the client. If a client computer were to provide a password on the list that was not the password associated with the particular password identifier, then the system in Heinz would reject access by the client computer. Heinz, therefore, is much less flexible than the invention of claim 1.

Furthermore, Heinz does not disclose or suggest receiving a numerical identifier from a requesting party, which obtained the numerical identifier from a transaction initiator claiming to

be associated with the numerical identifier. Rather, the client computer in Heinz claims to be associated with the password list of the registered user. The client computer in Heinz, therefore, is similar to the transaction initiator recited in claim 1 and cannot also function as the requesting party. The client computer in Heinz has no reason or motivation to verify its own identity. Such a characterization is nonsensical.

For at least these reasons, Heinz does not anticipate claim 1. Claims 2-4 and 11-13 depend from claim 1 and are allowable for at least the same reasons. Applicant does not otherwise concede the correctness of the rejection and reserves the right to make additional arguments if necessary.

Claim 14 recites, in part, a method of determining whether an identity verifier is required to be submitted in a particular transaction. The method includes creating categories of transactions and receiving instructions from a registered user designating the categories of transactions that require an identity verifier and designating the categories of transactions that do not require an identity verifier. The method further includes determining whether a transaction requires the use of an identity verifier.

Heinz fails to disclose or suggest creating categories of transactions. Applicants respectfully point out that Heinz's disclosure of dividing a password list into available and unavailable passwords is not equivalent to creating categories of transactions. Examples of transaction categories include checks under \$20 from a specific checking account and the use of a particular credit card. See, e.g., page 14, lines 27-29. Even if dividing a password list could be considered equivalent to creating categories of transactions, a point Applicants do not concede, no suggestion is made in Heinz to divide the list into such categories. Furthermore, Heinz does not disclose or suggest situations in which a transaction would not require an identity verifier. Rather, every transaction in Heinz appears to require a client to supply a password associated with a particular password identifier chosen by a server.

For at least these reasons, Heinz does not anticipate claim 14. Applicant does not otherwise concede the correctness of the rejection and reserves the right to make additional arguments if necessary.

Claim 15 recites, in part, an identity verification system for verifying the identity of a registered user. The verification system includes a communications module for receiving a numerical identifier and an identification verifier from a requesting party. The requesting party

obtained the numerical identifier and the identification verifier from a transaction initiator claiming to be associated with the numerical identifier and the identification verifier. The communications module also communicates a message to the requesting party relating to whether the received identification verifier is included on the list of identification verifiers linked to the received numerical identifier.

Heinz does not anticipate claim 15, therefore, for at least the same reasons as discussed above with respect to claim 1. Claims 16-19 depend from claim 15 and are allowable for at least the same reasons. Applicant does not otherwise concede the correctness of the rejection and reserves the right to make additional arguments if necessary.

Claim 20 recites, in part, a remote terminal for communicating with an identity verification system. The remote terminal includes an input module for inputting a numerical identifier and an identification verifier and a communications module for sending the numerical identifier and the identification verifier to a remotely located system. The communications module is also configured to receive from the remotely located system a security message linked with the identification verifier. The security message is a message provided by the registered user.

Heinz does not disclose or suggest a communications module configured to receive from a remotely located system a security message provided by the registered user and linked with the identification verifier. Furthermore, because the client computer in Heinz is equivalent to the registered user (or an identity thief masquerading as the registered user), the receipt of a security message provided by the registered user would be nonsensical. For at least these reasons, therefore, Heinz does not anticipate claim 20. Claims 21, 23, and 24 depend from claim 20 and are allowable for at least the same reasons. Applicant does not otherwise concede the correctness of the rejection and reserves the right to make additional arguments if necessary.

Claim 25 recites, in part, a computer program storage medium encoding a computer program for executing a computer process. The process includes receiving a numerical identifier and an identity verifier. The process further includes comparing the received numerical identifier and the received identity verifier to a stored numerical identifier and stored identity verifiers to determine whether the received identity verifier is one of the identity verifiers linked to the received numerical identifier. Heinz does not anticipate claim 25, therefore, for at least some of the reasons discussed above with respect to claim 1. Applicant does not otherwise

concede the correctness of the rejection and reserve the right to make additional arguments if necessary.

Claim 26 recites, in part, a method of verifying the identity of a registered user. The method includes receiving a numerical identifier and an identification verifier from a requesting party. The method further includes determining whether the identity verifier received from the requesting party is within a list of identity verifiers linked to the received numerical identifier. Heinz does not anticipate claim 26, therefore, for at least the same reasons as discussed above with respect to claim 1. Applicant does not otherwise concede the correctness of the rejection and reserves the right to make additional arguments if necessary.

### **Section 103 Rejections**

Applicant is confused regarding the rejection of claim 5. The rejection purports to reject claim 5 under 35 U.S.C. 103(a) as being unpatentable over Heinz as applied to claim 1, and further in view of Kuhns *et al.* However, the patent number given for the reference combined with Heinz is U.S. 6,047,281. This patent number is associated with a patent issued to Wilson *et al.* However, the Examiner refers to columns 16 and 17 when discussing the second reference cited in the obviousness rejection. Since columns 16 and 17 in the patent to Wilson include only the claims of Wilson, applicant assumes that the Examiner meant to reject claim 5 over Heinz in view of U.S. Patent No. 5,224,173 to Kuhns (previously cited). Applicant respectfully traverses the rejection.

Claim 5 depends from claim 1 and is allowable over Heinz for at least same reasons as discussed above with respect to claim 1. Kuhns does not overcome the shortcomings of Heinz. Kuhns does not disclose or suggest determining whether a received identity verifier is within a list of identity verifiers linked to a received numerical identifier. Rather, Kuhns is directed towards determining whether a scanned fingerprint is already stored within a central database.

Kuhns discloses associating certain physical characteristics of an applicant with the applicant's fingerprint. However, even if a fingerprint can be considered equivalent to the numerical identifier of claim 1, a point applicant does not concede, Kuhns still does not disclose determining whether the received identity verifiers are within the list of identity verifiers linked to the numerical identifier. Rather, Kuhns discloses weeding out fingerprints by first searching for matching physical characteristics. Neither the fingerprint nor the physical characteristics are

used for only one transaction. A user's fingerprints cannot change. Furthermore, prohibiting the use of the same physical characteristics when the characteristics of the user have not changed would interfere with the function of the invention disclosed in Kuhns.

In addition, the system in Kuhns does not communicate information to a requesting party indicating whether the physical characteristics are associated with a particular fingerprint. Rather, the system in Kuhns communicates a list of possible matches for the received fingerprint. Only one of these matches is actually associated with the registered user. Therefore, if the fingerprints disclosed in Kuhns are equivalent to the numerical identifiers of claim 1, then the purpose of the system disclosed in Kuhns functions merely to search for and identify a list of potential numerical identifier from a large list of numerical identifiers.

For at least these reasons, Heinz would not lead a person having skill in the art to the invention of claim 5, even in view of Kuhns. Applicant does not otherwise concede the correctness of the rejection and reserves the right to make additional arguments if necessary.

Claims 6 and 9 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Heinz as applied to claim 1, and further in view of Shkedy (U.S. 6,236,972, hereinafter "Shkedy"). Applicant respectfully traverses the rejection.

Claims 6 and 9 depend from claim 1 and are allowable over Heinz for at least the same reasons as discussed above with respect to claim 1. Shkedy does not overcome the shortcomings of Heinz. Rather, Shkedy is directed towards a system for buying and selling mutual funds. Shkedy does not provide much disclosure regarding verifying the identity of the parties. One example of a cryptographic process given in Shkedy includes performing a 512-bit NSA private key operation with a micro-controller. See, e.g., col. 9, lines 20-32. Public and private key cryptographic processes are known in the art and differ widely from the claimed invention. Generally, each private key corresponds with one public key. Furthermore, no motivation is provided in Shkedy to verify identity using the process disclosed in any of the pending claims. In particular, Shkedy does not disclose or suggest determining whether a received identity verifier is within a list of identity verifiers linked to a received numerical identifier.

For at least these reasons, therefore, Heinz would not lead a person having skill in the art to the invention of claim 1, even in view of Shkedy. Claims 6 and 9 are allowable for at least the same reasons. Applicant does not otherwise concede the correctness of the rejection and reserves the right to make additional arguments if necessary.

Claims 7, 8, and 10 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Heinz as applied to claim 1, and further in view of Gonzalo (U.S. 6,796,494, hereinafter "Gonzalo"). Applicant respectfully traverses the rejection.

Claims 7, 8, and 10 each depend from claim 1 and are allowable over Heinz for at least the same reasons as discussed above with respect to claim 1. Gonzalo does not overcome the shortcomings of claim 1. Gonzalo does not disclose how a customer's identity is verified. Rather, Gonzalo merely discloses that authorization can be based solely on information stored on an information card or information retrieved from a central server. See, *e.g.*, col. 4, lines 60-65. Gonzalo fails to disclose or suggest determining whether a received identity verifier is within a list of identity verifiers linked to a received numerical identifier.

For at least these reasons, Heinz would not lead a person having skill in the art to the invention of claim 1, even in view of Gonzalo. Claims 7, 8, and 10 depend from claim 1 and are allowable for at least the same reasons. Applicant does not otherwise concede the correctness of the rejection and reserve the right to make additional arguments if necessary.

Claim 22 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Heinz as applied to claim 20, and further in view of Henn (U.S. 5,770,844, hereinafter "Henn"). Applicant respectfully traverses the rejection.

Claim 22 depends from claim 20 and is allowable over Heinz for at least the same reasons as discussed above with respect to claim 20. Henn does not overcome the shortcomings of Heinz. Rather, Henn merely discloses conducting a security check to determine whether a chip card is a valid chip card. See, *e.g.*, column 4, lines 47-51. Henn fails to disclose or suggest a communications module configured to receive from a remotely located system a security message provided by the registered user and linked with the identification verifier.

For at least these reasons, Heinz would not lead a person having skill in the art to the invention of claim 20, even in view of Henn. Claim 22 is allowable for at least the same reasons. Applicant does not otherwise concede the correctness of the rejection and reserves the right to make additional arguments if necessary.

In view of the above amendments and remarks, Applicant respectfully requests a Notice of Allowance. If the Examiner believes a telephone conference would advance the prosecution of this application, the Examiner is invited to telephone the undersigned at the below-listed telephone number.

Respectfully submitted,

MERCHANT & GOULD P.C.  
P.O. Box 2903  
Minneapolis, Minnesota 55402-0903  
(612) 332-5300

Date: 21 October, 2005

2-W-7  
\_\_\_\_\_  
Brian H. Batzli  
Reg. No. 32,960  
BHB/JKS/jt